UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS

CHRISTOPHER BRADLEY, on behalf of himself and all others similarly situated, Plaintiff, v. **SET FORTH, INC.** and **CENTREX SOFTWARE, INC.**, Defendants.	Case No. 1:24-cv-11691 **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

Christopher Bradley ("Plaintiff"), through his attorneys, individually and on behalf of all others similarly situated, brings this Class Action Complaint against Defendants Set Forth, Inc. and Centrex Software, Inc. ("Set Forth" or "Defendants"), and their present, former, or future direct and indirect parent companies, subsidiaries, affiliates, agents, and/or other related entities. Plaintiff alleges the following on information and belief—except as to his own actions, counsel's investigations, and facts of public record.

NATURE OF ACTION

1. This class action arises from Defendants' failure to protect highly sensitive data.

2. Defendants are businesses that "provide cloud-based customer relationship management (CRM) solutions powered by the Set Forth platform."[1]

3. As such, Defendants store a litany of highly sensitive personal identifiable information ("PII") about their current and former consumers. But Defendants lost control over

[1] *Notice of Data Security Incident*, FORTH, https://www.setforth.com/notice-of-data-security-incident/ (last visited Nov. 13, 2024).

that data when cybercriminals infiltrated their insufficiently protected computer systems in a data breach (the "Data Breach").

4. It is unknown for precisely how long the cybercriminals had access to Defendants' network before the breach was discovered. In other words, Defendants had no effective means to prevent, detect, stop, or mitigate breaches of their systems—thereby allowing cybercriminals unrestricted access to their current and former consumers' PII.

5. On information and belief, cybercriminals were able to breach Defendants' systems because Defendants failed to adequately train their employees on cybersecurity and failed to maintain reasonable security safeguards or protocols to protect the Class's PII. In short, Defendants' failures placed the Class's PII in a vulnerable position—rendering them easy targets for cybercriminals.

6. Plaintiff is a Data Breach victim, having received a breach notice. He brings this class action on behalf of himself, and all others harmed by Defendants' misconduct.

7. The exposure of one's PII to cybercriminals is a bell that cannot be unrung. Before this data breach, their current and former consumers' private information was exactly that—private. Not anymore. Now, their private information is forever exposed and unsecure.

PARTIES

8. Plaintiff, Christopher Bradley, is a natural person and citizen of Florida where he intends to remain.

9. Defendant, Set Forth, Inc., is a corporation incorporated in Delaware and with its principal place of business at 1900 E Golf Road, Suite 550, Schaumburg, Illinois 60173.

10. Defendant, Centrex Software, Inc., is a stock corporation incorporated in California and with its principal place of business at 3090 Pullman Street, Costa Mesa, California 92626.

JURISDICTION AND VENUE

11. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. Plaintiff and Defendants are citizens of different states. And there are over 100 putative Class Members.

12. This Court has personal jurisdiction over Defendants because Set Forth, Inc. is headquartered in Illinois and because all Defendants regularly conduct business in Illinois and have sufficient minimum contacts in Illinois.

13. Venue is proper in this Court because Set Forth, Inc.'s principal office is in this District, and because a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in this District.

BACKGROUND

Defendants Collected and Stored the PII of Plaintiff and the Class

14. Defendants are businesses that "provide cloud-based customer relationship management (CRM) solutions powered by the Set Forth platform."[2]

15. As part of their business, Defendants receive and maintain the PII of thousands of their current and former consumers.

16. In collecting and maintaining the PII, Defendants agreed they would safeguard the data in accordance with their internal policies, state law, and federal law. After all, Plaintiff and Class Members themselves took reasonable steps to secure their PII.

[2] *Notice of Data Security Incident*, FORTH, https://www.setforth.com/notice-of-data-security-incident/ (last visited Nov. 13, 2024).

17. Under state and federal law, businesses like Defendants have duties to protect their current and former consumers' PII and to notify them about breaches.

18. Defendants recognizes these duties, declaring in their "Privacy Policy" that:

a. "Forth, Inc. (hereinafter 'Forth™' or 'Forth') is dedicated to protecting your privacy and providing you with the highest level of service."[3]

b. "To protect your personal information from unauthorized access and use, we use security measures that comply with federal law."[4]

c. "These measures include computer safeguards and secured files and buildings."[5]

d. "We also attempt to limit personal information access to only employees, agents and representatives who need to know."[6]

Defendants' Data Breach

19. On May 21, 2024, Defendants was hacked in the Data Breach.[7]

20. Because of Defendants' Data Breach, at least the following types of PII were compromised: "names, Social Security numbers, dates of birth, and addresses."[8]

[3] *Privacy Policy*, FORTH, https://www.setforth.com/privacy-policy/ (last visited Nov. 13, 2024).
[4] *Id*.
[5] *Id*.
[6] *Id*.
[7] *Notice of Data Security Incident*, FORTH, https://www.setforth.com/notice-of-data-security-incident/ (last visited Nov. 13, 2024).
[8] *Id*.

21. In total, Defendants injured at least 1,500,000 persons—via the exposure of their PII—in the Data Breach.[9] Upon information and belief, these 1,500,000 persons include their current and former consumers.

22. And yet, Defendants waited over until November 8, 2024, before they began notifying the class—a full 171 days after the Data Breach began.[10]

23. Thus, Defendants kept the Class in the dark—thereby depriving the Class of the opportunity to try and mitigate their injuries in a timely manner.

24. Defendants failed in their duties when their inadequate security practices caused the Data Breach. In other words, Defendants' negligence is evidenced by their failure to prevent the Data Breach and stop cybercriminals from accessing the PII. And thus, Defendants caused widespread injury and monetary damages.

25. Further, the Notice of Data Breach shows that Defendants cannot—or will not—determine the full scope of the Data Breach, as Defendants have been unable to determine precisely what information was stolen and when.

26. Defendants have done little to remedy their Data Breach. True, Defendants have offered some victims credit monitoring and identity related services. But upon information and belief, such services are wholly insufficient to compensate Plaintiff and Class Members for the injuries that Defendants inflicted upon them.

---

[9] *Data Breach Notifications*, MAINE ATTY GEN, https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/5c00fedb-134a-4436-b778-5df30b84cdab.html (last visited Nov. 13, 2024).

[10] *Notice of Data Security Incident*, FORTH, https://www.setforth.com/notice-of-data-security-incident/ (last visited Nov. 13, 2024).

27. Because of Defendants' Data Breach, the sensitive PII of Plaintiff and Class Members was placed into the hands of cybercriminals—inflicting numerous injuries and significant damages upon Plaintiff and Class Members.

28. Upon information and belief, the cybercriminals in question are particularly sophisticated. After all, the cybercriminals: (1) defeated the relevant data security systems, (2) gained actual access to sensitive data, and (3) successfully accessed data.

29. And as the Harvard Business Review notes, such "[c]ybercriminals frequently use the Dark Web—a hub of criminal and illicit activity—to sell data from companies that they have gained unauthorized access to through credential stuffing attacks, phishing attacks, [or] hacking."[11]

30. Thus, on information and belief, Plaintiff's and the Class's stolen PII has already been published—or will be published imminently—by cybercriminals on the Dark Web.

Plaintiff's Experiences and Injuries

31. Plaintiff Christopher Bradley is unsure how or why Defendants obtained—and then exposed—his PII.

32. Regardless, Defendants obtained and maintained Plaintiff's PII. As a result, Plaintiff was injured by Defendants' Data Breach.

33. Plaintiff (or his third-party agent) provided Defendants with his PII. Defendants used that PII to facilitate provision of services.

34. Plaintiff (or his third-party agent) provided his PII to Defendants and trusted the company would use reasonable measures to protect it according to Defendants' internal policies, as well as state and federal law. Defendants obtained and continues to maintain Plaintiff's PII and

[11] Brenda R. Sharton, *Your Company's Data Is for Sale on the Dark Web. Should You Buy It Back?*, HARVARD BUS. REV. (Jan. 4, 2023) https://hbr.org/2023/01/your-companys-data-is-for-sale-on-the-dark-web-should-you-buy-it-back.

has a continuing legal duty and obligation to protect that PII from unauthorized access and disclosure.

35. Plaintiff (or his third-party agent) reasonably understood that a portion of the funds paid to Defendants would be used to pay for adequate cybersecurity and protection of PII.

36. Plaintiff received a Notice of Data Breach on November 8, 2024.

37. Thus, on information and belief, Plaintiff's PII has already been published—or will be published imminently—by cybercriminals on the Dark Web.

38. Through their Data Breach, Defendants compromised Plaintiff's name, date of birth, address, and Social Security number.

39. Plaintiff has *already* suffered from identity theft and fraud when cybercriminals used Plaintiff's PII to sign up for a subscription in or around September 2024.

40. Plaintiff has spent—and will continue to spend—significant time and effort monitoring his accounts to protect himself from identity theft. After all, Defendants directed Plaintiff to take those steps in their breach notice.

41. And in the aftermath of the Data Breach, Plaintiff has suffered from a spike in spam and scam text messages and phone calls.

42. Plaintiff fears for his personal financial security and worries about what information was exposed in the Data Breach.

43. Because of Defendants' Data Breach, Plaintiff has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Plaintiff's injuries are precisely the type of injuries that the law contemplates and addresses.

44. Plaintiff suffered actual injury from the exposure and theft of his PII—which violates his rights to privacy.

45. Plaintiff suffered actual injury in the form of damages to and diminution in the value of his PII. After all, PII is a form of intangible property—property that Defendants was required to adequately protect.

46. Plaintiff suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Defendants' Data Breach placed Plaintiff's PII right in the hands of criminals.

47. Because of the Data Breach, Plaintiff anticipates spending considerable amounts of time and money to try and mitigate his injuries.

48. Today, Plaintiff has a continuing interest in ensuring that his PII—which, upon information and belief, remains backed up in Defendants' possession—is protected and safeguarded from additional breaches.

Plaintiff and the Proposed Class Face Significant Risk of Continued Identity Theft

49. Because of Defendants' failure to prevent the Data Breach, Plaintiff and Class Members suffered—and will continue to suffer—damages. These damages include, *inter alia*, monetary losses, lost time, anxiety, and emotional distress. Also, they suffered or are at an increased risk of suffering:

a. loss of the opportunity to control how their PII is used;

b. diminution in value of their PII;

c. compromise and continuing publication of their PII;

d. out-of-pocket costs from trying to prevent, detect, and recovery from identity theft and fraud;

e. lost opportunity costs and wages from spending time trying to mitigate the fallout of the Data Breach by, *inter alia*, preventing, detecting, contesting, and recovering from identify theft and fraud;

f. delay in receipt of tax refund monies;

g. unauthorized use of their stolen PII; and

h. continued risk to their PII—which remains in Defendants' possession—and is thus as risk for futures breaches so long as Defendants fails to take appropriate measures to protect the PII.

50. Stolen PII is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII can be worth up to $1,000.00 depending on the type of information obtained.

51. The value of Plaintiff and Class's PII on the black market is considerable. Stolen PII trades on the black market for years. And criminals frequently post and sell stolen information openly and directly on the "Dark Web"—further exposing the information.

52. It can take victims years to discover such identity theft and fraud. This gives criminals plenty of time to sell the PII far and wide.

53. One way that criminals profit from stolen PII is by creating comprehensive dossiers on individuals called "Fullz" packages. These dossiers are both shockingly accurate and comprehensive. Criminals create them by cross-referencing and combining two sources of data—first the stolen PII, and second, unregulated data found elsewhere on the internet (like phone numbers, emails, addresses, etc.).

54. The development of "Fullz" packages means that the PII exposed in the Data Breach can easily be linked to data of Plaintiff and the Class that is available on the internet.

55. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and Class Members, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff and other Class Members' stolen PII is being misused, and that such misuse is fairly traceable to the Data Breach.

56. Defendants disclosed the PII of Plaintiff and Class Members for criminals to use in the conduct of criminal activity. Specifically, Defendants opened up, disclosed, and exposed the PII of Plaintiff and Class Members to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen PII.

57. Defendants' failure to promptly and properly notify Plaintiff and Class Members of the Data Breach exacerbated Plaintiff and Class Members' injury by depriving them of the earliest ability to take appropriate measures to protect their PII and take other necessary steps to mitigate the harm caused by the Data Breach.

Defendants Knew—Or Should Have Known—of the Risk of a Data Breach

58. Defendants' data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in recent years.

59. In 2021, a record 1,862 data breaches occurred, exposing approximately

293,927,708 sensitive records—a 68% increase from 2020.[12]

60. Indeed, cyberattacks have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service issue warnings to potential targets, so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals . . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[13]

61. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendants' industry, including Defendant.

Defendants Failed to Follow FTC Guidelines

62. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. Thus, the FTC issued numerous guidelines identifying best data security practices that businesses—like Defendant—should use to protect against unlawful data exposure.

63. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*. There, the FTC set guidelines for what data security principles and practices businesses must use.[14] The FTC declared that, *inter alia*, businesses must:

a. protect the personal customer information that they keep;

b. properly dispose of personal information that is no longer needed;

---

[12] *See 2021 Data Breach Annual Report*, IDENTITY THEFT RESOURCE CENTER (Jan. 2022) https://notified.idtheftcenter.org/s/.

[13] Ben Kochman, *FBI, Secret Service Warn of Targeted Ransomware*, LAW360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware.

[14] *Protecting Personal Information: A Guide for Business,* FED TRADE COMMISSION (Oct. 2016) https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

64. The guidelines also recommend that businesses watch for the transmission of large amounts of data out of the system—and then have a response plan ready for such a breach.

65. Furthermore, the FTC explains that companies must:

a. not maintain information longer than is needed to authorize a transaction;

b. limit access to sensitive data;

c. require complex passwords to be used on networks;

d. use industry-tested methods for security;

e. monitor for suspicious activity on the network; and

f. verify that third-party service providers use reasonable security measures.

66. The FTC brings enforcement actions against businesses for failing to protect customer data adequately and reasonably. Thus, the FTC treats the failure—to use reasonable and appropriate measures to protect against unauthorized access to confidential consumer data—as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

67. In short, Defendants' failure to use reasonable and appropriate measures to protect against unauthorized access to their current and former consumers' data constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

Defendants Failed to Follow Industry Standards

68. Several best practices have been identified that—at a *minimum*—should be implemented by businesses like Defendant. These industry standards include: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption (making data unreadable without a key); multi-factor authentication; backup data; and limiting which employees can access sensitive data.

69. Other industry standard best practices include: installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

70. Upon information and belief, Defendants failed to implement industry-standard cybersecurity measures, including failing to meet the minimum standards of both the NIST Cybersecurity Framework Version 2.0 (including without limitation PR.AA-01, PR.AA.-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR-DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04) and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

71. These frameworks are applicable and accepted industry standards. And by failing to comply with these accepted standards, Defendants opened the door to the criminals—thereby causing the Data Breach.

CLASS ACTION ALLEGATIONS

72. Plaintiff brings this class action under Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3), individually and on behalf of all members of the following class:

> All individuals residing in the United States whose PII was compromised in the Data Breach discovered by Set Forth in May 2024, including all those individuals who received notice of the breach.

73. Excluded from the Class are Defendant, their agents, affiliates, parents, subsidiaries, any entity in which Defendants have a controlling interest, any Defendants officer or director, any successor or assign, and any Judge who adjudicates this case, including their staff and immediate family.

74. Plaintiff reserves the right to amend the class definition.

75. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of his claims on class-wide bases using the same evidence as would be used to prove those elements in individual actions asserting the same claims.

76. Ascertainability. All members of the proposed Class are readily ascertainable from information in Defendants' custody and control. After all, Defendants already identified some individuals and sent them data breach notices.

77. Numerosity. The Class Members are so numerous that joinder of all Class Members is impracticable. Upon information and belief, the proposed Class includes at least 1,500,000 members.

78. Typicality. Plaintiff's claims are typical of Class Members' claims as each arises from the same Data Breach, the same alleged violations by Defendant, and the same unreasonable manner of notifying individuals about the Data Breach.

79. Adequacy. Plaintiff will fairly and adequately protect the proposed Class's common interests. His interests do not conflict with Class Members' interests. And Plaintiff has retained counsel—including lead counsel—that is experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf.

80. Commonality and Predominance. Plaintiff's and the Class's claims raise predominantly common fact and legal questions—which predominate over any questions affecting individual Class Members—for which a class wide proceeding can answer for all Class Members. In fact, a class wide proceeding is necessary to answer the following questions:

a. if Defendants had a duty to use reasonable care in safeguarding Plaintiff's and the Class's PII;

b. if Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. if Defendants were negligent in maintaining, protecting, and securing PII;

d. if Defendants breached contract promises to safeguard Plaintiff and the Class's PII;

e. if Defendants took reasonable measures to determine the extent of the Data Breach after discovering it;

f. if Defendants' Breach Notice was reasonable;

g. if the Data Breach caused Plaintiff and the Class injuries;

h. what the proper damages measure is; and

i. if Plaintiff and the Class are entitled to damages, treble damages, and or injunctive relief.

81. Superiority. A class action will provide substantial benefits and is superior to all other available means for the fair and efficient adjudication of this controversy. The damages or other financial detriment suffered by individual Class Members are relatively small compared to the burden and expense that individual litigation against Defendants would require. Thus, it would

be practically impossible for Class Members, on an individual basis, to obtain effective redress for their injuries. Not only would individualized litigation increase the delay and expense to all parties and the courts, but individualized litigation would also create the danger of inconsistent or contradictory judgments arising from the same set of facts. By contrast, the class action device provides the benefits of adjudication of these issues in a single proceeding, ensures economies of scale, provides comprehensive supervision by a single court, and presents no unusual management difficulties.

FIRST CAUSE OF ACTION
Negligence
(On Behalf of Plaintiff and the Class)

82. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

83. Plaintiff and the Class (or their third-party agents) entrusted their PII to Defendants on the premise and with the understanding that Defendants would safeguard their PII, use their PII for business purposes only, and/or not disclose their PII to unauthorized third parties.

84. Defendants owed a duty of care to Plaintiff and Class Members because it was foreseeable that Defendants' failure—to use adequate data security in accordance with industry standards for data security—would compromise their PII in a data breach. And here, that foreseeable danger came to pass.

85. Defendants have full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and the Class could and would suffer if their PII was wrongfully disclosed.

86. Defendants owed these duties to Plaintiff and Class Members because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendants knew or should have known would suffer injury-in-fact from Defendants' inadequate security practices. After all, Defendants actively sought and obtained Plaintiff and Class Members' PII.

87. Defendants owed—to Plaintiff and Class Members—at least the following duties to:

a. exercise reasonable care in handling and using the PII in their care and custody;

b. implement industry-standard security procedures sufficient to reasonably protect the information from a data breach, theft, and unauthorized;

c. promptly detect attempts at unauthorized access;

d. notify Plaintiff and Class Members within a reasonable timeframe of any breach to the security of their PII.

88. Thus, Defendants owed a duty to timely and accurately disclose to Plaintiff and Class Members the scope, nature, and occurrence of the Data Breach. After all, this duty is required and necessary for Plaintiff and Class Members to take appropriate measures to protect their PII, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

89. Defendants also had a duty to exercise appropriate clearinghouse practices to remove PII they were no longer required to retain under applicable regulations.

90. Defendants knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the PII of Plaintiff and the Class involved an unreasonable risk of harm to Plaintiff and the Class, even if the harm occurred through the criminal acts of a third party.

91. Defendants' duty to use reasonable security measures arose because of the special relationship that existed between Defendants and Plaintiff and the Class. That special relationship

arose because Plaintiff and the Class (or their third-party agents) entrusted Defendants with their confidential PII, a necessary part of obtaining services from Defendant.

92. Under the FTC Act, 15 U.S.C. § 45, Defendants had a duty to use fair and adequate computer systems and data security practices to safeguard Plaintiff and Class Members' PII.

93. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect the PII entrusted to it. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendants' duty to protect Plaintiff and the Class Members' sensitive PII.

94. Defendants violated their duty under Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards as described in detail herein. Defendants' conduct was particularly unreasonable given the nature and amount of PII Defendants had collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

95. The risk that unauthorized persons would attempt to gain access to the PII and misuse it was foreseeable. Given that Defendants hold vast amounts of PII, it was inevitable that unauthorized individuals would attempt to access Defendants' databases containing the PII — whether by malware or otherwise.

96. PII is highly valuable, and Defendants knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PII of Plaintiff and Class Members' and the importance of exercising reasonable care in handling it.

97. Defendants improperly and inadequately safeguarded the PII of Plaintiff and the Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

98. Defendants breached these duties as evidenced by the Data Breach.

99. Defendants acted with wanton and reckless disregard for the security and confidentiality of Plaintiff's and Class Members' PII by:

a. disclosing and providing access to this information to third parties and

b. failing to properly supervise both the way the PII was stored, used, and exchanged, and those in their employ who were responsible for making that happen.

100. Defendants breached their duties by failing to exercise reasonable care in supervising their agents, contractors, vendors, and suppliers, and in handling and securing the personal information and PII of Plaintiff and Class Members which actually and proximately caused the Data Breach and Plaintiff and Class Members' injury.

101. Defendants further breached their duties by failing to provide reasonably timely notice of the Data Breach to Plaintiff and Class Members, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiff and Class Members' injuries-in-fact.

102. Defendants have admitted that the PII of Plaintiff and the Class was wrongfully lost and disclosed to unauthorized third persons because of the Data Breach.

103. As a direct and traceable result of Defendants' negligence and/or negligent supervision, Plaintiff and Class Members have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

104. And, on information and belief, Plaintiff's PII has already been published—or will be published imminently—by cybercriminals on the Dark Web.

105. Defendants' breach of their common-law duties to exercise reasonable care and their failures and negligence actually and proximately caused Plaintiff and Class Members actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their PII by criminals, improper disclosure of their PII, lost benefit of their bargain, lost value of their PII, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendants' negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

SECOND CAUSE OF ACTION
Breach of Implied Contract
(On Behalf of Plaintiff and the Class)

106. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

107. Plaintiff and Class Members either directly contracted with Defendants or Plaintiff and Class Members were the third-party beneficiaries of contracts with Defendant.

108. Plaintiff and Class Members (or their third-party agents) were required to provide their PII to Defendants as a condition of receiving services provided by Defendant. Plaintiff and Class Members (or their third-party agents) provided their PII to Defendants or their third-party agents in exchange for Defendants' services.

109. Plaintiff and Class Members (or their third-party agents) reasonably understood that a portion of the funds they paid would be used to pay for adequate cybersecurity measures.

110. Plaintiff and Class Members (or their third-party agents) reasonably understood that Defendants would use adequate cybersecurity measures to protect the PII that they were required to provide based on Defendants' duties under state and federal law and their internal policies.

111. Plaintiff and the Class Members (or their third-party agents) accepted Defendants' offers by disclosing their PII to Defendants or their third-party agents in exchange for services.

112. In turn, and through internal policies, Defendants agreed to protect and not disclose the PII to unauthorized persons.

113. In their Privacy Policy, Defendants represented that they had a legal duty to protect Plaintiff's and Class Member's PII.

114. Implicit in the parties' agreement was that Defendants would provide Plaintiff and Class Members (or their third-party agents) with prompt and adequate notice of all unauthorized access and/or theft of their PII.

115. After all, Plaintiff and Class Members (or their third-party agents) would not have entrusted their PII to Defendants (or their third-party agents) in the absence of such an agreement with Defendant.

116. Plaintiff and the Class (or their third-party agents) fully performed their obligations under the implied contracts with Defendant.

117. The covenant of good faith and fair dealing is an element of every contract. Thus, parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—and not merely the letter—of the bargain. In short, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to their form.

118. Subterfuge and evasion violate the duty of good faith in performance even when an actor believes their conduct to be justified. Bad faith may be overt or consist of inaction. And fair dealing may require more than honesty.

119. Defendants materially breached the contracts they entered with Plaintiff and Class Members (or their third-party agents) by:

a. failing to safeguard their information;

b. failing to notify them promptly of the intrusion into their computer systems that compromised such information.

c. failing to comply with industry standards;

d. failing to comply with the legal obligations necessarily incorporated into the agreements; and

e. failing to ensure the confidentiality and integrity of the electronic PII that Defendants created, received, maintained, and transmitted.

120. In these and other ways, Defendants violated their duty of good faith and fair dealing.

121. Defendants' material breaches were the direct and proximate cause of Plaintiff's and Class Members' injuries (as detailed *supra*).

122. And, on information and belief, Plaintiff's PII has already been published—or will be published imminently—by cybercriminals on the Dark Web.

123. Plaintiff and Class Members (or their third-party agents) performed as required under the relevant agreements, or such performance was waived by Defendants' conduct.

THIRD CAUSE OF ACTION
Invasion of Privacy
(On Behalf of Plaintiff and the Class)

124. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

125. Plaintiff and the Class had a legitimate expectation of privacy regarding their highly sensitive and confidential PII and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

126. Defendants owed a duty to their current and former consumers, including Plaintiff and the Class, to keep this information confidential.

127. The unauthorized acquisition (i.e., theft) by a third party of Plaintiff and Class Members' PII is highly offensive to a reasonable person.

128. The intrusion was into a place or thing which was private and entitled to be private. Plaintiff and the Class (or their third-party agents) disclosed their sensitive and confidential information to Defendant, but did so privately, with the intention that their information would be kept confidential and protected from unauthorized disclosure. Plaintiff and the Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

129. The Data Breach constitutes an intentional interference with Plaintiff's and the Class's interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

130. Defendants acted with a knowing state of mind when they permitted the Data Breach because they knew their information security practices were inadequate.

131. Defendants acted with a knowing state of mind when they failed to notify Plaintiff and the Class in a timely fashion about the Data Breach, thereby materially impairing their mitigation efforts.

132. Acting with knowledge, Defendants had notice and knew that their inadequate cybersecurity practices would cause injury to Plaintiff and the Class.

133. As a proximate result of Defendants' acts and omissions, the private and sensitive PII of Plaintiff and the Class were stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiff and the Class to suffer damages (as detailed *supra*).

134. And, on information and belief, Plaintiff's PII has already been published—or will be published imminently—by cybercriminals on the Dark Web.

135. Unless and until enjoined and restrained by order of this Court, Defendants' wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class since their PII are still maintained by Defendants with their inadequate cybersecurity system and policies.

136. Plaintiff and the Class have no adequate remedy at law for the injuries relating to Defendants' continued possession of their sensitive and confidential records. A judgment for monetary damages will not end Defendants' inability to safeguard the PII of Plaintiff and the Class.

137. In addition to injunctive relief, Plaintiff, on behalf of himself and the other Class Members, also seeks compensatory damages for Defendants' invasion of privacy, which includes the value of the privacy interest invaded by Defendant, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest and costs.

FOURTH CAUSE OF ACTION
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

138. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

139. This claim is pleaded in the alternative to the breach of implied contract claim.

140. Plaintiff and Class Members (or their third-party agents) conferred a benefit upon Defendant. After all, Defendants benefitted from (1) using their PII to provide services, and (2) accepting payment.

141. Defendants appreciated or had knowledge of the benefits they received from Plaintiff and Class Members (or their third-party agents).

142. Plaintiff and Class Members (or their third-party agents) reasonably understood that Defendants would use adequate cybersecurity measures to protect the PII that they were required to provide based on Defendants' duties under state and federal law and their internal policies.

143. Defendants enriched themselves by saving the costs they reasonably should have expended on data security measures to secure Plaintiff's and Class Members' PII.

144. Instead of providing a reasonable level of security, or retention policies, which would have prevented the Data Breach, Defendants instead calculated to avoid their data security obligations at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendants' failure to provide the requisite security.

145. Under principles of equity and good conscience, Defendants should not be permitted to retain the full value of Plaintiff's and Class Members' (1) PII and (2) payment because Defendants failed to adequately protect their PII.

146. Plaintiff and Class Members have no adequate remedy at law.

147. Defendants should be compelled to disgorge into a common fund—for the benefit of Plaintiff and Class Members—all unlawful or inequitable proceeds that they received because of their misconduct.

FIFTH CAUSE OF ACTION
Breach of Fiduciary Duty

(On Behalf of Plaintiff and the Class)

148. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

149. Given the relationship between Defendants and Plaintiff and Class Members, where Defendants became guardian of Plaintiff's and Class Members' PII, Defendants became a fiduciary by their undertaking and guardianship of the PII, to act primarily for Plaintiff and Class Members, (1) for the safeguarding of Plaintiff and Class Members' PII; (2) to timely notify Plaintiff and Class Members of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendants did and does store.

150. Defendants have a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of Defendants' relationship with them—especially to secure their PII.

151. Because of the highly sensitive nature of the PII, Plaintiff and Class Members (or their third-party agents) would not have entrusted Defendant, or anyone in Defendants' position, to retain their PII had they known the reality of Defendants' inadequate data security practices.

152. Defendants breached their fiduciary duties to Plaintiff and Class Members by failing to sufficiently encrypt or otherwise protect Plaintiff's and Class Members' PII.

153. Defendants also breached their fiduciary duties to Plaintiff and Class Members by failing to diligently discover, investigate, and give notice of the Data Breach in a reasonable and practicable period.

154. As a direct and proximate result of Defendants' breach of their fiduciary duties, Plaintiff and Class Members have suffered and will continue to suffer numerous injuries (as detailed *supra*).

SIXTH CAUSE OF ACTION
Violation of the Illinois Consumer Fraud and Deceptive Business Practices Act

815 ICLS 505/1, *et seq*.
(On Behalf of Plaintiff and the Class)

155. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

156. This claim is brought under the Illinois Consumer Fraud and Deceptive Business Practices Act ("ICFA").

157. Plaintiff and Class Members are "consumers" as defined in 815 Ill. Comp. Stat. § 505/1(e).

158. Plaintiff, the Class, and Defendants are "persons" as defined in 815 Ill. Comp. Stat. § 505/1(c).

159. The ICFA applies to Defendants because Defendants engaged in "trade" or "commerce," including the provision of services, as defined under 815 Ill. Comp. Stat. § 505/1(f). Defendants engages in the sale of "merchandise" (including services) as defined by 815 Ill. Comp. Stat. § 505/1(b) and (d).

160. Defendants violated ICFA by, *inter alia*:

a. failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Class Members' PII, which was a direct and proximate cause of the Data Breach;

b. failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e,

and the GLBA, 15 U.S.C. § 6801, *et seq*., which was a direct and proximate cause of the Data Breach;

d. omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiff's and Class Members' PII; and

e. omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq*.

161. Defendants' omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendants' data security and ability to protect the confidentiality of their PII.

162. Defendants intended to mislead Plaintiff and Class Members and induce them to rely on their omissions.

163. Had Defendants disclosed to Plaintiff and Class Members (or their third-party agents) that their data systems were not secure—and thus vulnerable to attack—Defendants would have been unable to continue in business and they would have been forced to adopt reasonable data security measures and comply with the law. Defendants accepted the PII that Plaintiff and Class Members (or their third-party agents) entrusted to them while keeping the inadequate state of their security controls secret from the public. Accordingly, Plaintiff and Class Members acted reasonably in relying on Defendants' omissions, the truth of which they could not have discovered through reasonable investigation.

164. Defendants acted intentionally, knowingly, maliciously, and recklessly disregarded Plaintiff's and Class Members' rights.

165. As a direct and proximate result of Defendants' unfair and deceptive acts and practices, Plaintiff and Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their PII.

166. And, on information and belief, Plaintiff's PII has already been published—or will be published imminently—by cybercriminals on the Dark Web.

167. Plaintiff and Class Members seek all monetary and non-monetary relief allowed by law.

168. Defendants' wrongful practices were and are injurious to the public because those practices were part of Defendants' generalized course of conduct that applied to the Class. Plaintiff and the Class have been adversely affected by Defendants' conduct and the public was and is at risk as a result thereof.

169. Defendants also violated 815 ILCS 505/2 by failing to immediately notify Plaintiff and the Class of the nature and extent of the Data Breach pursuant to the Illinois PII Protection Act, 815 ILCS 530/1, *et seq*.

170. Pursuant to 815 Ill. Comp. Stat. § 505/10a(a), Plaintiff and the Class seek actual and compensatory damages, injunctive relief, and court costs and attorneys' fees as a result of Defendants' violations of the ICFA.

SEVENTH CAUSE OF ACTION
Declaratory Judgment

(On Behalf of Plaintiff and the Class)

171. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

172. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary relief. The Court has broad authority to restrain acts, such as those alleged herein, which are tortious and unlawful.

173. In the fallout of the Data Breach, an actual controversy has arisen about Defendants' various duties to use reasonable data security. On information and belief, Plaintiff alleges that Defendants' actions were—and *still* are—inadequate and unreasonable. And Plaintiff and Class Members continue to suffer injury from the ongoing threat of fraud and identity theft.

174. Given its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendants owed—and continues to owe—a legal duty to use reasonable data security to secure the data entrusted to it;

b. Defendants have a duty to notify impacted individuals of the Data Breach under the common law and Section 5 of the FTC Act;

c. Defendants breached, and continues to breach, their duties by failing to use reasonable measures to the data entrusted to it; and

d. Defendants' breaches of their duties caused—and continues to cause—injuries to Plaintiff and Class Members.

175. The Court should also issue corresponding injunctive relief requiring Defendants to use adequate security consistent with industry standards to protect the data entrusted to it.

176. If an injunction is not issued, Plaintiff and the Class will suffer irreparable injury and lack an adequate legal remedy if Defendants experiences a second data breach.

177. And if a second breach occurs, Plaintiff and the Class will lack an adequate remedy at law because many of the resulting injuries are not readily quantified in full and they will be forced to bring multiple lawsuits to rectify the same conduct. Simply put, monetary damages—while warranted for out-of-pocket damages and other legally quantifiable and provable damages—cannot cover the full extent of Plaintiff and Class Members' injuries.

178. If an injunction is not issued, the resulting hardship to Plaintiff and Class Members far exceeds the minimal hardship that Defendants could experience if an injunction is issued.

179. An injunction would benefit the public by preventing another data breach—thus preventing further injuries to Plaintiff, Class Members, and the public at large.

PRAYER FOR RELIEF

Plaintiff and Class Members respectfully request judgment against Defendants and that the Court enter an order:

A. Certifying this case as a class action on behalf of Plaintiff and the proposed Class, appointing Plaintiff as class representative, and appointing his counsel to represent the Class;

B. Awarding declaratory and other equitable relief as necessary to protect the interests of Plaintiff and the Class;

C. Awarding injunctive relief as necessary to protect the interests of Plaintiff and the Class;

D. Enjoining Defendants from further unfair and/or deceptive practices;

E. Awarding Plaintiff and the Class damages including applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

F. Awarding restitution and damages to Plaintiff and the Class in an amount to be determined at trial;

G. Awarding attorneys' fees and costs, as allowed by law;

H. Awarding prejudgment and post-judgment interest, as provided by law;

I. Granting Plaintiff and the Class leave to amend this complaint to conform to the evidence produced at trial; and

J. Granting other relief that this Court finds appropriate.

DEMAND FOR JURY TRIAL

Plaintiff demands a jury trial for all claims so triable.

Dated: November 13, 2024

By: */s/ Samuel J. Strauss*

Samuel J. Strauss
Raina C. Borrelli
STRAUSS BORRELLI PLLC
One Magnificent Mile
980 N Michigan Avenue, Suite 1610
Chicago IL, 60611
Telephone: (872) 263-1100
Facsimile: (872) 263-1109
sam@straussborrelli.com
raina@straussborrelli.com

Attorneys for Plaintiff and the Proposed Class

Date: November 13, 2024

Respectfully submitted,

By: /s/ *Samuel J. Strauss*

Samuel J. Strauss
Raina C. Borrelli*
STRAUSS BORRELLI PLLC
980 N. Michigan Avenue, Suite 1610
Chicago, Illinois 60611
T: (872) 263-1100
F: (872) 263-1109
sam@straussborrelli.com
raina@straussborrelli.com

**Pro hac vice forthcoming*
Attorneys for Plaintiff and Proposed Class